HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400, BOX 1000
APO AE 09128

PAMPHLET
NUMBER 25-2

25 January 2001

SECURITY

Security Awareness

---

1. **Purpose**. This pamphlet serves as an integral part of your security indoctrination training for your assignment with Headquarters United States European Command (HQ USEUCOM) or one of its assigned elements. It is designed to:

a. Advise you of the adverse effects to national security that could result from any unauthorized disclosure, and of your personal, moral, and legal responsibility to protect classified information within your possession, or control.

b. Familiarize you with the principles, criteria, and procedures for the classification, downgrading, declassification, marking, control, accountability, storage, destruction, and transmission of any classified information or material, and alert you to the strict prohibitions on improper abuse of the classification system.

c. Familiarize you with required procedures for classification challenges, if any observed classification decisions are believed to be improper.

d. Familiarize you with the security requirements of your new assignment.

e. Inform you of the techniques employed by foreign intelligence activities in attempting to obtain classified information, and your responsibility to report any such attempts.

f. Advise you of the penalties for engaging in espionage activities.

g. Advise you of the strict prohibition against discussing classified information over an unsecured telephone or in any other manner that permits interception by unauthorized persons.

h. Inform you of the penalties for violating the provisions of DOD 5200.1-R, Information Security Program Regulation.

This Pamphlet supersedes EP 25-2, dated 16 Jul 96

i. Explain to you that before individuals can have knowledge, possession, or control of classified information, you must determine the following before disseminating such information: a prospective recipient is cleared for access by competent authority; needs the information in order to perform official duties, and; can properly protect the information.

2. **Applicability**. This pamphlet applies to all HQ USEUCOM personnel assigned to directorates, staff offices, and direct reporting units, regardless of location.

3. **Internal Control Systems**. This pamphlet contains internal control provisions and is subject to the requirements of the internal management control program. For HQ USEUCOM and subordinate activities, the applicable internal control directive is ED 50-8, Internal Management Control Program.

4. **Suggested Improvements**. The proponent for this Pamphlet is the Office of the Special Assistant for Security Matters. Suggestions for any improvements should be forwarded to HQ USEUCOM, ATTN: ECSM, Unit 30400, Box 1000, APO AE 09128.

5. **Reference**. Department of Defense 5200.1-R, Information Security Program Regulation.

6. **Responsibilities**. Protection and proper control of classified national defense information is an inherent responsibility of all members of the Department of Defense. The Office of the Special Assistant for Security Matters manages the HQ USEUCOM Information Security Program for collateral security issues. Each directorate and staff office has a "Security Manager" responsible for administering programs within their respective organizations.

7. **Summary**. You are a vital link to having a sound information security program. Your security manager and ECSM stand ready and able to advise and/or assist you in all security or related matters. Remember, protecting classified or sensitive information is everyone's responsibility.

FOR THE COMMANDER-IN-CHIEF:

OFFICIAL:

DANIEL J. PETROSKY
Lieutenant General, USA
Chief of Staff

DAVID R. ELLIS
Lieutenant Colonel, USA
Adjutant General

APPENDICES
A - Safeguarding Defense Information
B - Classification Principles, Criteria, Considerations, and Designations
C - Marking Documents
D - Classification Challenges
E - Security Training Requirements
F - The Hostile Threat
G - Telephone Security
H - Administrative Sanctions
I - Security Clearances and Access

DISTRIBUTION:
P

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

Safeguarding Defense Information

1. HQ USEUCOM is a unified/combatant command and a dedicated member of the North Atlantic Treaty Organization Alliance. Our job is vital to the national defense effort. As a member of this command, you will be entrusted with highly sensitive and classified information. Therefore it is a foregone conclusion that a compromise of such information would be detrimental to the interests of the United States and would have an adverse affect upon our national security. You have a moral, legal, and personal responsibility to protect classified information of which you have knowledge, possession, or control.

2. Classified documents must never be left unattended. Whenever offices are left unoccupied, all classified material must be properly secured. This is true even if the office is unattended for only a short period of time, such as for lunch or a distribution run. Leaving classified material in an unattended office and locking the door is NOT authorized.

3. At the close of each working day, you may be appointed by the directorate/staff office chief to conduct an area security check. You will be responsible for ensuring that all classified material, including waste, is properly stored or destroyed; wastebaskets do not contain classified material; all security containers have been locked; and Standard Forms 701, Activity Security Checklist, and 702, Security Container Check Sheet, have been properly annotated.

4. Rules for protecting classified information/material apply equally to all material, regardless of whether the information is contained in traditional paper documents or in secure computer systems. When computers are not located in SCIFs or properly approved "open storage areas", hard-drives and other removable media MUST be secured in GSA approved security containers when not under the direct supervision of a properly cleared and duly authorized person.

5. Prior to allowing uncleared personnel access to "open storage" or other areas where classified information is processed, you must ensure the area is sanitized, to include covering classified materials when personnel are working or securing materials in a safe. For "open storage" approved areas, uncleared personnel MUST BE ESCORTED AT ALL TIMES.

6. DO NOT remove classified materials from security containers unless you are working on them. Limit removal of documents for work to the minimum required at one time. At the end of the duty day, you should have a "clean desk policy" for your office to facilitate identification of classified information that requires securing prior to your departure.

7. This guidance applies equally to all assigned personnel; however, it applies specifically to collateral/genser classified information. For personnel working with Sensitive Compartmented Information (SCI) or other special access programs (SAP), coordinate classification and declassification needs with the original classifier, derivative classifier, your local special security office, or program manager for the SAP. Sensitive Compartmented Information (SCI) is information that requires special controls and restricted access due to its sensitive nature. It is all information and material, which because of its source or subject matter, requires limited access and restricted handling in special "channels" or "compartments". To ensure this category of information is protected properly, contact the USEUCOM Special Security Office for assistance.

APPENDIX B

Classification Principles, Criteria, Considerations, and Designations

1. Under Executive Order 12958, there are three levels of classification for U.S. information: Top Secret, Secret and Confidential.

a. Top Secret information is information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

b. Secret information is information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

c. Confidential information is information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

2. Original classification is the initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. Only select senior officials are delegated original classification authority. Original classification authority is used only in those instances when any security classification guide does not cover the information. A guide should cover the vast majority of cases. Put a different way, original classification means taking a piece of information that has never been classified and making it classified. In order to limit the number of original classification decisions that need to be made, classification guides should be identified, or developed by the directorate/staff office with original classification authority over the information. (NOTE: If there is significant doubt about the need to originally classify information, do not classify.) To be eligible for original classification, information must fall within one or more of the following categories of information listed in section 1.5 of Executive Order 12958:

(1) Military plans, weapons systems, or operations.

(2) Foreign government information.

(3) Intelligence activities (including special activities), intelligence sources or methods, or cryptology.

(4) Foreign relations or foreign activities of the United States, including confidential sources.

(5) Scientific, technological, or economic matters relating to the national security.

(6) United States Government programs for safeguarding nuclear materials or facilities.

(7) Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

c. Information may not be classified for the purpose of:

(1) Concealing violations of law, inefficiency, or administrative error.

(2) Preventing embarrassment to a person, organization, or agency.

(3) Restraining competition.

(4) Preventing or delaying the release of information that does not require protection in the interest of national security.

(5) Basic scientific research information not clearly related to the national security may not be classified.

(6) Information may not be reclassified after it has been declassified and officially released to the public.

d. The ability to identify or describe the damage to national security is critical to making a classification decision. The original classification authority is not required to prepare a written account of the damage at the time of the decision to classify, but must be able to do so if the classified information becomes the subject of a classification challenge or a request for access (for example, under the Freedom of Information Act or the Privacy Act).

3. Derivative Classification. The majority of employees in the DOD community are derivative classifiers. This means you incorporate, paraphrase, restate, or generate in new form information that is already classified. As a derivative classifier, you refer to some sort of classification guidance (usually a classified source document, such as a regulation of OPLAN, or a classification guide) and mark newly developed materials consistent with the markings on the source or the instructions in the guide.

a. There are two common scenarios you will encounter in doing derivative classification:

(1) Sometimes, you will be copying, restating or paraphrasing information from a single classified document as you prepare your new document. In this case, you will put markings on your new document consistent with those found on the source document. If you use classified information from more than one source document, be careful to mark your new document with the highest classification of any of the information you used. If you have any doubt about the proper classification to use, check the security classification guide covering the subject, if one exists.

(2) In other situations, you will be creating a document without taking information from source documents. Here, you'll check the appropriate classification guide for instructions.

(3) A third scenario is much less common. If the information you're using is neither covered by a classification guide nor extracted from a classified source document, you're probably looking at a situation where original classification should be considered. You would assign the information a temporary (tentative) classification, and refer the matter to the appropriate original classification authority for a decision.

b. In doing derivative classification, you will need to understand the levels of classification, what may and may not be classified, classification guides, duration of classification, and document marking.

c. Classification Guides: As a derivative classifier, you will regularly refer to one or more classification guides to identify information that must be classified and the appropriate level and duration of classification. Classification guides provide comprehensive, detailed, authoritative guidance for frequently recurring items of sensitive information. Each organization with original classification authority will prepare and distribute its own guides. When USEUCOM organizations develop a classification guide, a copy should be provided to ECSM (Command Security Manager) for inclusion in appropriate files and/or coordinating with the Defense Technical Information Center for inclusion in their database. Copies of most guides in DOD are available from the Defense Technical Information Center.

(1) A classification guide states the following:

(a) Which classification level applies to each item of information and, when useful, specify items of information that are unclassified.

(b) Precisely which elements of information are to be protected?

(c) Provides a concise reason for classification. The guide must always cite the appropriate classification category from Section 1.5 of the E.O 12958.

(d) Provides information about special handling caveats, when appropriate.

(e) Prescribes declassification instructions or the automatic declassification exemption category for each element of information.

(f) States the date the guide was issued or last reviewed.

(2) Classification guides are updated as necessary and reviewed at least every five years.

(3) Contact ECSM for training on how to develop classification guidance, if required.

4. Declassification is the authorized changing of information from classified to unclassified.

a. When information is originally classified, the classifier must identify a date or event upon which the information will be declassified. The standard in Executive Order 12958 is that information should normally remain classified for no longer than 10 years. However, it also recognizes there are some circumstances in which information must stay classified longer than 10 years, because disclosure would cause damage to national security even after 10 years.

b. The original classification authority may exempt information from the 10-year rule if the disclosure would be expected to:

(1) Reveal an intelligence source, method or activity, or a crypto logic system or activity (X1)

(2) Reveal information that would assist in the development or use of weapons of mass destruction (X2)

(3) Reveal information that would impair the development or use of technology within a United States weapons system (X3)

(4) Reveal United States military plans or national security emergency preparedness plans (X4)

(5) Reveal foreign government information (X5)

(6) Damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period longer than 10 years (X6)

(7) Impair the ability of responsible United States Government officials to protect the President, the Vice-President, and other individuals for whom protection services, in the interest of national security, are authorized (X7)

(8) Violate a statute, treaty, or international agreement (X8)

c. The designators in parentheses following each item show the exemption categories specified in Section 1.6.d of Executive Order 12958.

5. Other Declassification Programs. You most likely won't be responsible for making declassification decisions, but you should understand the three separate programs for declassification established by the Executive Order 12958, are as follows:

a. Automatic Declassification. Unless an agency head takes specific action to extend the duration of classification, information 25 years old and older in records that have permanent historical value will be declassified automatically. Classification duration may be extended beyond 25 years only under certain narrowly defined conditions. Material that is exempted from this 25-year rule is still subject to the following declassification programs.

b. Systematic Review. This is a review for possible declassification of information contained in records that have been determined by the Archivist of the United States to have permanent historical value. Both the National Archives and Records Administration and individual agencies will be conducting review programs focused on records with substantial historical interest.

c. Mandatory Review. This is a review for possible declassification performed in response to a request received from an organization or an individual.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C

Marking Documents

1. Marking is our normal means of communicating the need to protect information. Markings must be uniformly and conspicuously applied to documents to leave no doubt as to the classification level, the reason for classification, the duration of classification, and the authority or source for classification. Proper markings are required for both hard-copy and electronic classified documents. In this appendix we'll quickly review some of the basic marking requirements. Other markings may be required, depending on the nature of the information and the type of document you're working with.

a. Portion Markings: Mark each portion of a document (normally paragraphs, but also including subjects, titles, charts, etc.) to indicate which portions are classified and at what level, and which portions are unclassified. To indicate the classification level, you use the symbols (TS) for Top Secret, (S) for Secret, (C) for Confidential, and (U) for Unclassified.

b. Document and Page Markings: Mark the document conspicuously with the highest level of classification contained in the document. For example, if a document contained some Secret information and some Confidential information, the overall marking would be Secret. This marking must be placed at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). Interior pages of classified documents must also be marked.

c. Source of Classification and Declassification Instructions: Executive Order 12958 requires each classified document to be marked with certain information about the source or authority for classification, duration of classification, etc. Two or more of the following lines will appear on the face of a classified document, each of which may end up being more than a single line long. You must place the following information on the face of a classified document:

(1) Sometimes abbreviations are used, and may vary slightly. (Generally, use "Classified by (*or* CL BY): _____.) When used on originally classified documents, this line will identify the original classifier, either by name and position title or a personal identifier.

(2) Give the reason for classifying the information, citing the categories from section 1.5 of the Order. For example, this line might read 1.5(a). You may also cite more than one reason, e.g., 1.5(b), (c), and (d).

(3) Include the line "Derived from (or DRV FROM): _____". This line is to be used

on derivatively classified documents. On the line, place the title and date of the classification guidance you used (source document or classification guide). If you use more than one source document, classification guide, or combination of the two, this line should read Multiple Sources. You must identify each source used in a list maintained with the file or record copy of the document.

(4) Also, include "Declassify on (or DECL ON): _____". This line provides instructions for declassification of the information in both originally and derivatively classified documents. What you will place on this line will vary with your situation. It must contain a date or event for declassification or a marking showing it's exempt from the order's 10-year rule (for example, X7). Your security manager or security staff can help you determine exactly how to complete this line on your documents.

APPENDIX D

Classification Challenges

If you see a document you believe has been improperly classified, what should you do? E.O. 12958 has established guidelines for formally challenging the classification assigned to information. The Order states that those who challenge a classification will be protected from retribution. In fact, you are encouraged and expected to challenge the classification of information if you believe it is improper. Before resorting to the formal challenge procedures, an attempt should be made to resolve the matter informally. At USEUCOM, the following criteria applies:

a. Challenges must be in writing and described sufficiently to permit identification of the information or document being challenged and the classifier thereof;

b. All challenges regarding USEUCOM originated information will be submitted to your security manager;

c. A response to the challenge from the originator shall occur within sixty days of receipt. You will be notified of the results of the challenge.

THIS PAGE INTENTIONALLY LEFT BLANK

Security Training Requirements

1. In addition to this pamphlet, you will be receiving indoctrination training from your Directorate/Staff Security Manager and supervisor. They will provide you with information on the basic security requirements necessary for you to perform your particular assigned duties.

2. Upon completion of your briefings, you should familiarize yourself with DOD 5200.1R, Information Security Program Regulation, as supplemented, ED 25-1, USEUCOM Information Security Operating Instruction, and other security regulations required to perform your specific duties.

3. If you are a supervisor, remember that you are responsible for supporting your directorate/staff security manager in the training of assigned personnel and enforcement of security rules and regulations.

THIS PAGE INTENTIONALLY LEFT BLANK

The Hostile Threat

1. Allied personnel stationed abroad remain the focus of foreign intelligence efforts. The information most desired covers every aspect of this command's operations and administration. You will have access, in varying degrees, to this information. Because of this, you could be a target of a foreign intelligence agent.

2. Because all of us have information of potential interest to our adversaries, we must constantly be on the alert to deny them this information. We must remind others within the organization of their responsibility for safeguarding sensitive and classified information. We must help one another to be security conscious. You must report to the Stuttgart Area Military Intelligence Detachment or Air Force OSI anything of a suspicious nature involving personnel or information. Make every effort to remember as many details as possible and include them in your report. Report the following situations as soon as possible:

a. Attempts to obtain military information through observation, collection of documents, personal contact, coercion, or intimidation;

b. Attempts by individuals with foreign backgrounds or associations to cultivate friendships or to place personnel under obligation for the purpose of obtaining information.

c. If you have any questions concerning your responsibility to report, or if you feel an attempt has been made to obtain military information, contact your supervisor, your directorate/staff agency security manager, local military intelligence unit, or the HQ USEUCOM security manager.

THIS PAGE INTENTIONALLY LEFT BLANK

Telephone Security

1. Our telephone calls are subject to monitoring by foreign intelligence services. Therefore, it is paramount that classified or sensitive information not be discussed over non-secure telephones. When you have to discuss this type of information, always use a STU-III or other secure communications device.

2. Do not try to double talk; that is, talk around the subject. This practice could result in a violation. Persons violating telephone security procedures are subject to disciplinary action.

3. Another concern is discussion of sensitive information in public places. Your Operations Security Officer will provide you with the "tools" needed to recognize and understand sensitive issues. Remember that common sense and sound security awareness should prevail at all times.

4. DO NOT TAKE CELL PHONES, RADIOS, OR OTHER COMMUNICATIONS DEVICES into SCIFs, or other areas where classified discussions and processing take place. Prior to commencing classified briefings, conferences, or other discussions, double check to ensure these devices are not in the area. In some instances, powering down the device and removing the battery will suffice, however, check with the SCIF or secure area custodian for additional guidance.

THIS PAGE INTENTIONALLY LEFT BLANK

Sanctions

1. Military and civilian personnel of the Department of Defense are responsible individually for complying with the provisions of DOD 5200.1-R, as supplemented, and taking all necessary precautions to protect sensitive and unclassified National Defense Information. Failure to do so will subject the offender to administrative and/or criminal sanctions.

a. You are subject to administrative and criminal sanctions if you: knowingly, willfully, or negligently: classify or continue the classification of information improperly classified under relevant legal guidance such as Executive Order 12958 or DoD 5200.1-R; disclose to unauthorized persons properly classified information; create or continue a Special Access Program contrary to applicable regulation; or if you violate any other provision or reference to DOD 5200.1R.

b. Accordingly, repeated administrative discrepancies in the marking and handling of classified documents and material, such as failure to show classification authority, failure to apply internal classification markings, and incorrect declassification instructions, or other repeated disregard of requirements that are determined to constitute a violation, are grounds for adverse administrative or criminal action against the offender.

c. In cases of demonstrated reckless disregard or a pattern of error in applying applicable classification standards on the part of the person holding original classification authority, the offending individual original classification authority shall be removed by the appropriate official.

d. Administrative Sanctions: Administrative sanctions include, but are not limited to, a warning notice, a reprimand, termination of classification authority, suspension without pay, forfeiture of pay, removal, discharge, and loss or denial of access to classified information.

e. Criminal Sanctions: Criminal Sanctions include offenses under the Uniform Code of Military Justice (UCMJ) or Federal criminal code law should actions constitute a violation of those codes. Potential offenses under the UCMJ are: Espionage (Article 106a, UCMJ), Spying (Article 106, UCMJ), Destruction, sale, loss, damage or wrongful disposition of Military (or other) Property of the United States, (Articles 106, 109, respectively, UCMJ). Potential Federal code offenses are Gathering, Transmitting, or Losing Defense Information in violation of 18 USC 793, and Gathering, or Delivering Defense Information to Aid Foreign Governments in violation of 18 USC 794. Civilians, in times of war, could be charged under the UCMJ for spying, while military members could be charged with Federal code offenses under the third clause of Article 134, UCMJ.

2. Illustrative Examples: The two examples noted below involve one of the provisions of 18 USC 793, section (f) which notes:

Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, or appliance, note or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer,

Shall be fined under this title or imprisoned not more than ten years.

Example 1: An Air Force member intermingled two classified messages with personal mail he was carrying to a friend in Prudhow Bay. Alaska. On arrival, some 725 miles away from his duty station, the member discovered he had inadvertently brought these two TOP SECRET messages with him. He placed them in a desk drawer in his friend's room, intending to pick them up later and return them to his squadron. After the weekend, he returned to his duty station, forgetting the documents. His friend's roommate found the papers in the desk drawer, and gave them to his supervisor. The court found the member effectively had lost the documents, and affirmed his sentence of a bad conduct discharge, confinement for 43 days, and reduction to airman basic.

Example 2: A Marine member, responsible for all the "cod word" and other classified material n his unit, was convicted of violating this provision when we stored classified information in his desk located in an authorized SCIF. On his last day at work, he hastily packed his gym bag with material from his desk, when he discovered the material he inadvertently took, he stored it in a garage drawer, intending to destroy it at his new duty station. Te movers discovered the material, and turned the classified materials over to the NIS. The court found that he had a continuing duty to safeguard the information when he discovered he had taken it through gross negligence. His sentence as approved was confinement for ten months, a dishonorable discharge, and $400.00 per month for 36 months.

THIS PAGE INTENTIONALLY LEFT BLANK

Security Clearances and Access

1. The HQ USEUCOM ECJ2-SSO Personnel Security Section is the only security clearance authority for this command. Clearances are granted upon completion of proper investigation, review of pertinent records, and continued qualification for access to classified information while assigned to this command. Your supervisor will determine and control the degree of access you require. Once again, you'll be called upon to report any information concerning security risks or anyone whose actions indicate the individual may be, or may become, a security risk. Additionally, you must report all known facts that bring to question reliability, trustworthiness, character, or judgment.

2. No person may have access to classified information unless the USEUCOM Personnel Security Section has granted that person local access. No one has a right to have access to classified information solely by virtue of rank or position. The final responsibility for determining whether an individual's official duties require possession of, or access to, and whether the individual has been granted, the appropriate security clearance, rests upon the individual who has authorized possession, knowledge, or control of the information.

THIS PAGE INTENTIONALLY LEFT BLANK